UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA
AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

IN THE MATTER OF THE SEARCH OF: INFORMATION ASSOCIATED WITH DISCORD ACCOUNTS: User ID's: 574774417838833688 and 269803120656252929 located on the servers at Discord 401 California Dr Burlingame, CA 94010	Case No. 3:19mj336

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Patrick Wilhelm, a Special Agent (SA) with Homeland Security Investigations (HSI), being duly sworn, depose and state as follows:

INTRODUCTION

1. I make this Affidavit in support of an Application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Discord to disclose to the government records and other information, including the contents of communications, associated with the above-listed account user name that is stored at premises owned, maintained, controlled, or operated by Discord. The information to be disclosed by Discord and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am a Special Agent with the United States Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI). I have been so employed from December 2003, to the present. I am currently assigned to HSI Charlotte, North Carolina office. As part of my

duties and responsibilities as an HSI Special Agent, I am authorized to investigate crimes involving the sexual exploitation of children pursuant to Title 18, United States Code, Section 2251, et seq. As part of my official duties, I have investigated criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251(a) and 2252A. I am also a computer forensic agent, trained to obtain electronic evidence from computers and other electronic storage media. Through the course of my job as a Special Agent and a computer forensics agent, I have viewed tens of thousands of images depicting child pornography (as defined in 18 U.S.C. § 2256) in various forms of media including computer media. In addition, I have received formal training from both ICE and other organizations in the area of child pornography and child exploitation investigations. I have also participated in the execution of numerous search warrants, many of which involved child exploitation and/or child pornography offenses.

3. This affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the locations specifically described in **Attachment A** of this Affidavit, including the contents of the Discord accounts with user ID's 574774417838833688 and 269803120656252929 (herein after referred to as SUSPECT USER ACCOUNTS) that is stored at the premises owned, maintained, controlled, or operated by, Discord, 401 California Dr, Burlingame, CA 94010. Discord is a company that provides remote computing and electronic communications services. This affidavit is made in support of an application for search warrant to look for contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2251, 2252, and 2252A, which items are more specifically described in **Attachment B** of this Affidavit.

4. The statements in this affidavit are based on information provided by other law enforcement investigators involved in the investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§2251, 2252(a)(1) and (b)(1) (transportation of a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252(a)(2) and (b)(1) (receipt/distribution of a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252A(a)(1) and (b)(1) (transportation of child pornography); 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) (receipt/distribution of child pornography); and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography), are presently located in the SUSPECT USER ACCOUNTS.

STATUTORY AUTHORITY

5. As noted above, this investigation concerns alleged violations of the following:

a. Title 18, United States Code, Sections 2251, 2252A(a)(1) and (b)(1) prohibit a person from knowingly mailing or transporting or shipping using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography, as defined in 18 U.S.C. § 2256(8), or attempting or conspiring to do so.

b. Title 18, United States Code, Sections 2252(a)(2) and (b)(1) prohibit any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer.

c. Title 18, United States Code, Sections 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

d. Title 18, United States Code, Section 2251 states that it is an offense when any person who employs, uses, persuades, induces, entices, or coerces any minor to engage in, or who has a minor assist any other person to engage in, or who transports any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, shall be punished as provided under subsection (e), if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or

mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed.

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachment B:

a. "Anime," as used herein, refers to refers to Japanese-style cartoon animation that is characterized by colorful graphics, vibrant characters, and fantastical themes, which may or may not include depictions of minors engaged in sexually explicit conduct.

b. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. See 18 U.S.C. § 1030(e)(1).

e. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

f. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched.

Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. "File Transfer Protocol" ("FTP") is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP, built on client-server architecture, uses separate control and data connections between the client and the server.

h. A "hash value" is a unique alpha-numeric identifier for a digital file. A hash value is generated by a mathematical algorithm, based on the file's content. A hash value is a file's "digital fingerprint" or "digital DNA." Two files having identical content will have the same hash value, even if the file names are different. On the other hand, any change to the data in a file, however slight, will change the file's hash value, even if the file name is unchanged. Thus, if two files have the same hash value, they are said to be identical, even if they have different file names.

i. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (ISPs) control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs

typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

j. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

k. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

l. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

m. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

n. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

o. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

p. A "website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language ("HTML") and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol ("HTTP").

q. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

DISCORD ACCOUNTS & SERVICES

7. Discord provides free hosting for registered users to set up, configure, and customize their own communication servers, as well as user text chat rooms. Discord is a web-based service which can be accessed via web browser or by installing an application for a Windows, iOS, or Android device. Users register for the service with an email address, username, and password; after registering users have access to all of Discords' features, including voice calls and chat rooms. Discord is an instant messaging service that provides both text and voice communication. Discord conversation logs are saved to a "Chats" area in the user's Discord account. Discord account users can link other social media and entertainment services to their Discord account and can automatically integrate features of those applications such as Google+. Discord stores identifying information (such as email address used to register

an account and a history of IP addresses), and usage information (such as chat logs, login sessions, and device information). Discord also collects information from any third-party application linked to a user's profile. The user account for a Discord account is alphanumeric username, which is then combined with a pound symbol (#) as well as a string of 4 or 5 randomized numbers, producing a unique "tag." The tag is publicly visible on an account's profile and can be used for a variety of networking purposes inside of Discord, such as friend lists, server whitelists, and blocking other users.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO ADVERTISE, TRANSPORT, DISTRIBUTE, RECEIVE, POSSESS, AND/OR ACCESS WITH INTENT TO VIEW CHILD PORNOGRAPHY

8. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who transport, distribute, receive, possess, and/or access with intent to view child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials or purchase childlike sex objects for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of

children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

f. Such individuals also may correspond with and/or meet others to share

information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses (including e-mail addresses), and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if Laws, or his affiliates, use a portable device (such as a mobile phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found in the SUSPECT DISCORD ACCOUNTS as set forth in Attachment A.

h. Such individuals, especially those utilizing cryptocurrency, and those who may have more knowledge and access to networks of other child pornography collectors and distributors, may be utilizing the dark web to access and purchase child pornography.

9. Based on the following, I believe that the users utilizing the SUSPECT DISCORD ACCOUNTS, likely display characteristics common to individuals who transport, distribute, possess or access with intent to view child pornography.

BACKGROUND ON CHILD PORNOGRAPHY, AND THE USE OF ELECTRONIC STORAGE AND EMAIL

10. I have had both training and experience in the investigation of internet related crimes. Based on my training, experience, and knowledge, I know the following:

a. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

b. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where an individual uses online storage, however, law enforcement can find evidence of child pornography on the user's computer, smartphone or external media in most cases.

c. As is the case with most digital technology, communications by way of email can be saved in their inbox or stored on a computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information such as the traces of the path of an electronic communication may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information exists indefinitely until overwritten by other data.

d. Individuals who use email to obtain child pornography often have saved contacts or communication via that email account with others who may be sharing, receiving or advertising child pornography.

PROBABLE CAUSE

10. On or about January 23, 2019 Google became aware of an account containing child pornography. The content was stored in Google Photos Infrastructure. The account name was Nick Wilde, the mobile phone associated with the account was listed as +13364523746 and the email address was claws8747@gmail.com. Google reported the child pornography to the National Center for Missing and Exploited Children's Cyber Tipline and was assigned a Cyber Tip number of 45949286. The National Center for Missing and Exploited Children (NCMEC) sent the Cyber Tip to the North Carolina State Bureau of Investigation (NCSBI.) Included in the Cyber Tip were IP addresses used to log into Google and an image of two nude prepubescent males engaged in sexual activity. Agents from the NCSBI sent an administrative subpoena to Century Links legal department for the IP address of 76.2.46.84. The IP address resolved to Linda Laws, 428 Noah Harrold Rd, Hays, NC.

11. On May 7, 2019 investigators with the NCSBI and Wilkes County Sheriff's Office conducted a knock and talk at 428 Noah Harrold Rd, Hays, NC. Present at the residence was Christopher Laws. Laws voluntarily spoke with the investigators. He stated he lived at this residence with his grandmother. Laws told the investigators his mobile number was 336-452-3746 and one of his email accounts was claws8747@gmail.com and one of the names he used was Nick Wilde. Laws stated he used multiple email addresses to log into an application named Discord where he would trade images and videos of child pornography with other users. Additionally, Laws stated he used the email address of chrislaws15@gmail.com and names "blood wolf" and "wolfy" in the Discord app where he would upload and send the images and videos. Laws stated he had more than one Discord account. Furthermore, Laws stated he used an application named

Mega to store the images and videos for the purpose of encrypting the media. Finally, Laws stated he would trade images and videos daily through the Discord app.

12. On this same date while investigators spoke with Laws he gave his permission for them to preview his mobile phone. NCSBI Special Agent Chambliss observed several images consistent with child pornography on the mobile phone, as well as the Discord app with identifiable user information. NCSBI seized the phone for the purposes of forensic analysis.

13. On August 1, 2019 United States Magistrate Judge Keesler issued a search warrant to Homeland Security Investigations SA Swafford for Discord records affiliated with Laws' Discord user name of "wolfy#6377". Discord returned information requested in the search warrant which contained communications between Laws and other Discord users which included, but was not limited to, other Discord user ID's, user names, shared images, chats, and shared links between Discord users. Although there were many user ID's affiliated with the Discord chat group Laws participated in, investigative efforts at this time have identified two user ID's that received child pornography from Laws. The Discord user ID's 574774417838833688 and 269803120656252929 received child pornography from Laws between May 7-9, 2019. Specifically, Laws sent Discord user 574774417838833688 a .jpg photo depicting a nude female toddler approximately 2 to 4 years of age appearing to be faced down on a bed with a nude adult male penetrating the female toddler's vagina. In addition to the photo, Laws sent an .mp4 video approximately 34 seconds in length of a female toddler nude from the waist down. In the video an adult male is depicted straddling the female toddler's face, holding the toddler's right buttock, and penetrating the female toddler's vagina with his penis. Also, during this same time frame Laws sent Discord user 269803120656252929 a .jpg photo

depicting a nude female infant approximately 2 to 4 months of age with an adult male penis penetrating the infant's vagina. In addition to the photo, Laws sent an .mp4 video approximately 1 minute and 25 seconds in length depicting an approximately 5 to 8 years of age nude female with an adult male penetrating the child's vagina with his penis.

14. Based on the facts that Discord files containing easily accessible communications between Laws and other SUSPECT DISCORD ACCOUNTS showing Laws distributed files containing child pornography to those accounts, there is probable cause to believe the Discord accounts 574774417838833688 and 269803120656252929, which are affiliated with the Discord chat group Laws participated in, may contain evidence of violations of the above enumerated statutes, namely 18 U.S.C. 2251 and 2252A.

SPECIFICS OF SEARCH AND SEIZURE OF DISCORD ACCOUNT(S)

15. Information stored in connection with a Discord account may provide crucial evidence of the "who, what, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. Stored electronic communications, and other data retained by Discord, can indicate who has used or controlled the Discord account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, emails, chat logs, and files interacted with may be evidence of who used or controlled the Discord account at a relevant time. Further, Discord account activity can show how and when the account was accessed or used. For example, Discord logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses; investigators can

understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Discord account access, use, and events relating to the crime under investigation. Last, Discord account activity may provide relevant insight into the Discord account owner's state of mind as it relates to the offense under investigation. For example, information on the Discord account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

15. Therefore, the account servers of Discord are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Discord, such as account access information, transaction information, and other account information.

16. Because the warrant will be served on Discord who will then compile the requested records at a time convenient to Discord, reasonable cause exists to support execution of the requested warrant at any time day or night.

REQUEST FOR SEALING OF WEBSITE/AFFIDAVIT

17. It is respectfully requested that this Court issue an order sealing, until further order of this Court, all papers submitted in support of this Application, including the Application, Affidavit, and Search Warrant, and the requisite inventory notice. Sealing is necessary because the items and information agents intend to seize are relevant to an ongoing investigation and agents will not search all the targets of this investigation at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and

search warrants via the Internet and disseminate them to other online criminals as they deem appropriate, *i.e.*, post them publicly online through forums. Premature disclosure of the contents of this Affidavit and related documents may have a significant and negative impact on this continuing investigation and may jeopardize its effectiveness by alerting potential targets to the existence and nature of the investigation, thereby giving them an opportunity to flee, or to destroy or tamper with evidence.

18. Notwithstanding 18 U.S.C. § 2252/2252A or any similar statute or code, Discord shall disclose responsive data by sending it to: HSI Special Agent Walter L. Swafford, 3700 Arco Corporate Dr, Ste 300, Charlotte, NC, 28273; or via email to walter.l.swafford@ice.dhs.gov.

CONCLUSION

19. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that the Discord accounts with user ID's 574774417838833688 and 269803120656252929 located on servers at Discord, 401 California Dr, Burlingame, CA, have been used to distribute child pornography in violation of 18 U.S.C. §§ 2251(a), 2252(a), and 2252A(a).

20. Further, there is probable cause to believe that evidence, fruits, and instrumentalities of such criminal offenses may be found in Discord records.

21. I, therefore, respectfully request that that attached warrant be issued authorizing the search and seizure of the items listed in **Attachment B**.

Patrick Wilhelm
Special Agent,
Homeland Security Investigations

this 24th day of September 2019.

David Keesler
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED

This warrant applies to information associated with the Discord accounts with User ID's 574774417838833688 and 269803120656252929 which is stored at premises owned, maintained, controlled, or operated by Discord headquartered at 401 California Drive, Burlingame, California 94010.

ATTACHMENT B

PROPERTY TO BE SEARCHED AND/OR SEIZED

This warrant authorizes (i) the search of the property identified in Attachment A for only the following and (ii) authorizes the seizure of the items listed below only to the extent they constitute the following:

(a) evidence of violations of 18 U.S.C. §§ 2251, 2252 and 2252A ("subject violations"); or

(b) any item constituting contraband due to the subject violations, fruits of the subject violations, or other items possessed whose possession is illegal due to the subject violations; or

(c) any property designed for use, intended for use, or used in committing any subject violations.

Subject to the foregoing, the items authorized to be seized include the following:

I. Information to be disclosed by Discord.

To the extent that the information described in Attachment A is within the possession, custody, or control of Discord, including any emails, chats, images, records, files, logs, or information that have been deleted but are still available to Discord, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Discord is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all chats associated with the account, including stored or preserved copies of chats sent to and from the account, the source and destination addresses associated with each chat, the date and time at which each chat was sent, and the size and length of each chat;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates,

account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between Discord, and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252A, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. All images depicting children engaging in sexually explicit conduct as defined in 18 U.S.C. § 2256

b. All electronic communications regarding children engaging in sexually explicit conduct;

c. All communications with potential minors involving sexual topics or in an effort to seduce the minor.

d. Any evidence that would tend to identify the person using the account when any of the items listed in subparagraphs a-c were sent, read, copied or downloaded.

e. Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.